

Q2 Public Sector

Quarterly Threat Landscape Scorecard

TLP: WHITE S-2022-08-05a



Q2 2022 Public Sector Threat Overview

Threat actors continued to exchange ideas on how to maneuver within the economic and political constraints brought about by the conflict in Ukraine in Q2. Public sector organizations faced a persistent threat from social engineering campaigns, with particularly increases in the use of fraudulent applications, fake Windows 11 upgrades, and employment-related scams to steal credentials and deploy trojans. The threat of vulnerability exploitation grew, averaging almost 70 Common Vulnerabilities and Exposures (CVEs) disclosed per day—up from 56 per day at the end of 2021. The pace of vulnerability disclosure likely represents a new normal. The threat to the public sector from Initial Access Brokers (IABs) continued to fall in Q2, despite the market showing signs of resurgence in other sectors.

Although spyware received significant media attention in Q2 2022—in particular, long-standing targeting of high-profile public sector individuals globally—this likely represents little change in the scale of threat posed. The threat from ransomware and digital extortion likely increased, with multiple central government and local government entities targeted. Ransomware threat actors may be struggling to elicit payments from victims, driving changes to extortion tactics. Lastly, while the ongoing war in Ukraine continued to be the primary driver of geopolitical risk, possible EU and NATO expansion—and new sanctions on Russia—will likely trigger Russian-leaning groups to target high-profile entities.

Key Cyber Threats to the Public Sector in Q2 2022



State-linked and financially motivated threat actors targeting key personnel, including in job-related scams



Vulnerabilities in third-party software used by public sector organizations and the pace of exploitation



Ransomware and digital extortion outfits conducting high-profile attacks against public sector and government entities



Changes to extortion tactics resulting in greater operational downtime, reputational damage, and legal ramifications



Spyware deployed against high-profile public sector personnel



Saturated infostealer and trojan markets, with releases of new strains and old strains updating capabilities



Russia-backed and aligned threat actors targeting high-profile public sector entities



Malware disguised in applications targeting employees and members of the public

Public Sector Threats*

Categories	Q1 2022	Q2 2022
Social Engineering		
Vulnerability Exploitation		
Initial Access Brokers		
Botnets		
Malware		
Ransomware		

KEY

Indication of decrease in threat from previous quarter

No notable change in threat from previous quarter

Indication of increase in threat from previous quarter

> Q2 Key Findings:

- Cybercriminals are concerned with challenges converting cryptocurrency to fiat currency.
- Social engineering campaigns increasingly used LNK shortcut files, fake Windows upgrades, and employment scams.
- The threat from CVEs and previously-unknown software vulnerabilities likely increased.
- The threat from IABs continued to fall in the public sector in Q2, despite the IAB market showing signs of resurgence in threats to other sectors.
- Although spyware received significant media attention in Q2—in particular, long-standing targeting of high-profile public sector individuals globally—this likely represents little change in the scale of threat posed.
- The threat to public sector organizations from ransomware and digital extortion likely increased. Eliciting payment from victims may be getting more difficult.

*ZeroFox acknowledges the variation in entities classified as public sector depending on the country in question. For the purpose of this report, "public sector" refers to all public sector entities within the United States and all formal branches of government in other countries.

SCOPE NOTE

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 5:00 PM (EDT) on July 21, 2022; per cyber hygiene best practices, caution is advised when clicking on any third-party links.



SOCIAL ENGINEERING

Social engineering campaigns continued to impersonate and target public sector entities and representatives, leveraging malicious email attachments. This quarter saw increased use of LNK files. While the overall threat remained broadly consistent, ZeroFox Intelligence observed an increase in fraudulent applications, fake Windows 11 upgrades, and employment-related scams to deploy banking trojans and infostealers.

Forward Look:

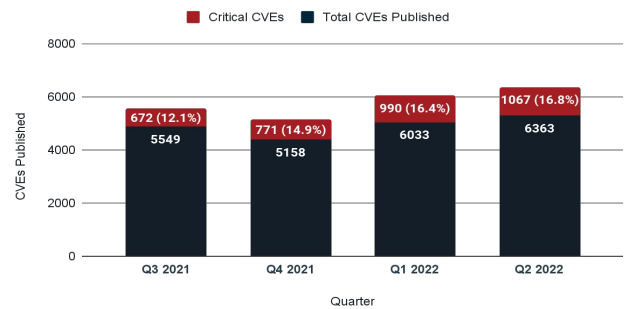
- Job-related scams will target desirable employees at a high pace, particularly those with elevated access levels.
- Fake applications will increasingly be used to target customers.
- Malicious email attachments will continue to be used to disseminate malware.

Recommendations:

- Communicate to prospective candidates what legitimate job postings look like to get ahead of fake offers.
- Engage ZeroFox Intelligence to conduct an Attack Surface Assessment to understand the threat posed to your organization.

No notable change in threat from previous quarter

Total CVEs Published by Quarter



Source: [hXXps://nvd.nist.gov](https://nvd.nist.gov)

VULNERABILITY EXPLOITATION

Public sector entities faced an unprecedented threat from disclosed vulnerabilities, particularly in cloud and network perimeter infrastructure—including routers, firewalls, and commonly-used software modules. The importance of efficient patching was magnified by widespread reporting of vulnerabilities, enabling threat actors to rapidly target vulnerable systems.

Forward Look:

- Vulnerabilities in the cloud and network perimeter infrastructure will likely continue to dominate the exploit landscape.
- The scale and pace of exploit disclosures likely represent a new normal for the vulnerability landscape.

Recommendations:

- Use the ZeroFox Platform's Intelligence Search capability to investigate Vulnerabilities and associated Exploits.
- Ensure a thorough understanding of your technology stack and patching schedule, as well as those of operating partners.

Indication of increase in threat from previous quarter

INITIAL ACCESS BROKERS

The threat to the public sector from IABs continued to fall in Q2, despite the IAB market showing signs of resurgence in threats to other sectors. Advertisements focused on entities participating in high-profile events. Threats often trend against particular industries for a period of time before moving on and spiking against others. Disruption to IAB operations is keeping supply below 2021 levels.

Forward Look:

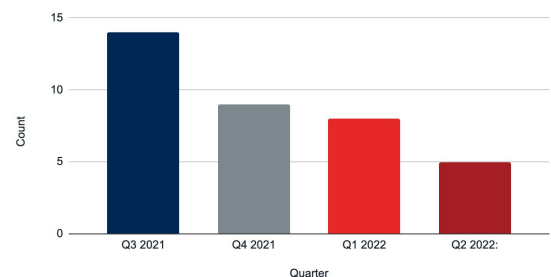
- The threat from IABs will likely increase given strong demand from buyers and disruption to IAB operations likely being temporary.
- Threat actors may be increasingly pushed to more private means to sell illicit access, making identifying activity more difficult.

Recommendations:

- Employ ZeroFox Threat Intelligence Feeds to get ahead of threat actor activity.
- Proactively monitor for potential network access sales to obtain critical early warnings of impending cyberattacks.

Indication of decrease in threat from previous quarter

Advertised IAB Access into Public Sector Organizations by Quarter



Source: ZeroFox Intelligence

FOOTNOTES

[hXXps://blog.malwarebytes.com/scams/2022/04/usps-your-package-could-not-be-delivered-text-is-a-smishing-scam/](https://blog.malwarebytes.com/scams/2022/04/usps-your-package-could-not-be-delivered-text-is-a-smishing-scam/)
[hXXps://www.bleepingcomputer.com/news/security/windows-zero-day-exploited-in-us-local-govt-phishing-attacks/](https://www.bleepingcomputer.com/news/security/windows-zero-day-exploited-in-us-local-govt-phishing-attacks/)
[hXXps://www.cert.gov.ng/advisories/hackers-using-fake-windows-11-upgrade-to-install-malware-steals-information](https://www.cert.gov.ng/advisories/hackers-using-fake-windows-11-upgrade-to-install-malware-steals-information)
[hXXps://www.zdnet.com/article/security-researchers-heres-how-the-lazarus-hackers-start-their-attacks/](https://www.zdnet.com/article/security-researchers-heres-how-the-lazarus-hackers-start-their-attacks/)
[hXXps://nvd.nist.gov](https://nvd.nist.gov)
 ZeroFox Intelligence Internal Collections



BOTNETS

Most public sector bodies around the world saw a negligible change in the threat from botnets in Q2 2022. Russia-aligned groups began targeting entities in countries that vocally opposed the war in Ukraine with botnet attacks, though not at the scale or breadth expected. Botnets deploying infostealers continued to pose a high threat to public sector organizations. Public sector bodies should note Emotet's resurgence which, at its peak, was one of the largest and most capable botnets in history.

Forward Look:

- Botnets leveraged by Russia-aligned entities could exacerbate geopolitical tensions.
- The continued resurgence of Emotet indicates it may pose a significant threat to public sector entities around the world in the coming months.

Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate network and infrastructure Indicators of Compromise (IOCs) of interest, including C2 Domains and Compromised Account Credentials. Proactive monitoring of botnet logs provides critical early warning of impending cyberattacks.

No notable change in threat from previous quarter

RANSOMWARE

The threat to the public sector from ransomware and digital extortion likely increased in Q2 2022, with a higher frequency of attacks—particularly against local governments—and threat actors demonstrating greater capability than in Q1 2022 attacks. Multiple high-profile attacks targeted government entities in Q2 2022. Threat actors may be struggling to elicit payments from victims, driving changes to extortion tactics.

Forward Look:

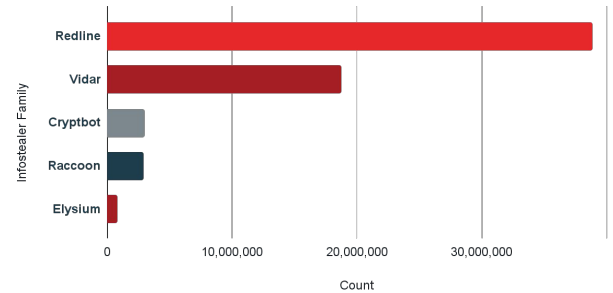
- ZeroFox Intelligence anticipates the threat to public sector entities will most likely increase.
- Threat actors may resort to more extreme pressure tactics to elicit payment from victims that cause greater operational downtime, reputational damage, and legal ramifications.

Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate IOCs and metadata related to Malware and Ransomware.
- Should an organization be impacted by a ransomware event, engage ZeroFox Intelligence for support.

Indication of increase in threat from previous quarter

Q2 2022: Credentials Ingested from Information Stealer Families Commonly Used by Botnets



Source: ZeroFox Intelligence

MALWARE

The threat from malware deployment across the landscape remained high in Q2 2022. The threat to public sector organizations was underpinned by the high rate of new infostealers and trojans emerging and older versions launching new campaigns. There was likely little change to the threat posed by spyware, with the greatest threat to the public sector coming from fraudulent apps distributing spyware modules. However, Q2 highlighted the threat spyware poses to high-profile individuals in the public sector and the importance of good security practices in mitigating any attempted attacks.

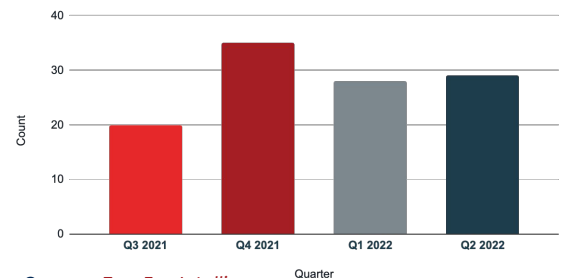
Forward Look:

- Malware-as-a-service offerings will very likely sustain low barriers to entry for threat actors and drive down the price of acquiring highly-capable malware.
- Rapid modification to trojans to exploit newly disclosed vulnerabilities will place increased importance on having a robust patching program.

Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate IOCs and metadata related to Malware and Ransomware.

Total Public Sector Ransomware and Digital Extortion Events by Quarter



Source: ZeroFox Intelligence

FOOTNOTES

<https://www.politico.eu/article/russia-hackers-killnet-attack-lithuania-over-kaliningrad-sanction/>
<https://www.theregister.com/2022/06/10/emotet-malware-chrome-credit-cards/>
<https://thehackersnews.com/2022/05/over-200-apps-on-play-store-caught.html>
<https://thehackersnews.com/2022/06/nso-confirms-pegasus-spyware-used-by-at.html>
<https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/>
<https://securityaffairs.it/wordpress/132122/cyber-crime/city-of-palermo-vice-society-ransomware.html>



QUARTERLY SPOTLIGHT

In Russian-language Deep and Dark Web forums, the fate of cryptocurrency and strategies to exchange crypto for fiat currency are increasing concerns, particularly because many cybercriminals see cryptocurrencies as the only means of transferring financial support to Russia. We expect cyber actors to pivot and adapt in near real-time to offset temporary disruptions to their financial gains, likely relying on institutions in geopolitically indifferent or supportive countries. They will also very likely continue to seek methods that use stable financial institutions, exchanging rubles for cryptocurrency that can then be converted to hard currency—most likely U.S. dollars—and offshored to non-Russian banks for safety.

APPENDIX: Traffic Light Protocol for Information Dissemination

TLP : RED

HOW IT IS USED

Sources may use TLP: **RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW IT IS SHARED

Recipients may NOT share TLP: **RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

TLP : AMBER

HOW IT IS USED

Sources may use TLP: **AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW IT IS SHARED

Recipients may ONLY share TLP: **AMBER** information with members of their own organization and only as widely as necessary to act on that information.

TLP : GREEN

HOW IT IS USED

Sources may use TLP: **GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW IT IS SHARED

Recipients may share TLP: **GREEN** information with peers & partner organizations within their sector or community but not via publicly accessible channels.

TLP : WHITE

HOW IT IS USED

Sources may use TLP: **WHITE** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW IT IS SHARED

Recipients may share TLP: **WHITE** information without restriction, subject to copyright controls.

OUTLOOK

Russia's invasion of Ukraine will likely continue to heavily influence the cyber threat landscape. The conflict and resulting humanitarian and economic crises will almost certainly continue to be leveraged by threat actors in social engineering lures. Vulnerabilities in cloud infrastructures, perimeter security devices, and commonly-used software modules will also likely continue to dominate the exploit landscape. ZeroFox Intelligence anticipates pro-Russia threat actors and state-linked entities will likely increasingly target countries and organizations with malware in retaliation for perceived stances taken during the war.

If ransomware operators struggle to elicit payments from victims, it is likely they will resort to more extreme pressure tactics, threatening to cause greater operational downtime, reputational damage, and legal ramifications.

ZEROFOX INTELLIGENCE
August 5, 2022

ABOUT ZEROFOX

ZeroFox provides enterprises protection, intelligence, and disruption to dismantle external threats to brands, people, assets, and data across the public attack surface in one comprehensive platform. With complete global coverage across the surface, deep, and dark web and an Intel-backed artificial intelligence-based analysis engine, the ZeroFox Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, ransomware, brand hijacking, executive and location threats, and more.

The patented ZeroFox Platform technology processes and protects millions of posts, messages, and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, domains, cloud-based email, and more.

READY TO SEE FOR YOURSELF?

> Request a Demo:

Sign up on zerofox.com/request-a-demo

> Learn More:

Visit zerofox.com

Contact us at sales@zerofox.com / 855.736.1400

